Towards Quantifying the Impacts of Cyber Attacks in the Competitive Electricity Market Environment

by: Matias Negrete-Pincetic, Felipe Yoshida and George Gross
Department of Electrical and Computer Engineering
University of Illinois at Urbana-Champaign

Presenter: Karanvir Kaleka

Submitted in Partial Fulfillment of the Course Requirements for
ECEN 689: Cyber Security of the Smart Grid
Instructor: Dr. Deepa Kundur

Outline

- Introduction
- Types of attacks
- Real examples of vulnerabilities & cyber attacks
- Proposed framework
- Simulation results
- Conclusion

Introduction and Motivation

- Power grid is a critical infrastructure of our modern society
  - 2003 blackout affected 50 million people and cost ~6-13 billion dollars
- Increasing complexity has resulted in the use of more wireless communications, Supervisory Control and Data Acquisition (SCADA) control systems, and the internet
  - Adds to the already known physical vulnerabilities
- There needs to be a way of characterizing cyber attacks and quantifying their economic impacts
- Electricity industry is made up of 3 levels
  - Physical, Communication/Control, and Market
- In addition to these, proposed framework also includes a fourth cyber security investment layer

Types of Attacks

- Denial of Service (DoS)
- Replay
- Man-in-the-middle
- Reprogramming RTUs

➢ Each of these attacks are capable of compromising one or more of the following SCADA information security goals:

  – Confidentiality, Integrity, and Availability

Types of Attacks, Cont'd

Attack type		DoS	Replay	Man-in-the-middle	Reprogramming RTUs
Objective		Make a resource temporarily unavailable	"listen", identify, and replay a message at an opportune time to repeat a previous action	Trick the sender (receiver) believe he is the correct receiver(sender)	Reprogram RTUs to insert malicious behavior
Compromises		Availability	Confidentiality & Integrity	Confidentiality & Integrity	Confidentiality & Integrity
Difficulty		Low	Medium	High	Highest
Outcome	**Most Likely**	Temporary and local loss of connection	Temporary blackouts	-	-
	Worst Case	All communication is disabled, emergency situation will not be realized	Permanent damage can be done if EMS does not take the required actions	Emergency messages from RTU could be intercepted and retransmitted as if everything is OK	If successful, attacker would have complete control over the reprogrammed RTUs

Vulnerabilities and Attack Examples

TEXAS A&M UNIVERSITY

- Aurora Test
- Ira-Winkler
- TVA (Tennessee Valley Authority)
- Hatch-power plant

Aurora Test

- Who: Department of Energy (DOE) Idaho Lab
- When: March, 2007
- What: DOE launched an experimental cyber attack on the replica of a power plant control system and caused a generator to self-destruct.

http://www.youtube.com/watch?v=fJyWngDco3g&feature=related

Ira-Winkler

- Who: Security consultant Ira Winkler & team
- When: April, 2008
- What: As part of penetration-testing, experts were able to hack into a power company network in less than a day. In addition to overseeing the power production and distribution, they could also download the CIO and CEO records.

TVA

- Who: Government Accountability Office
- When: March, 2008
- What: GAO reports that nation's largest publicly owned utility company TVA vulnerable to cyber attacks which could disrupt the system and cause a blackout.

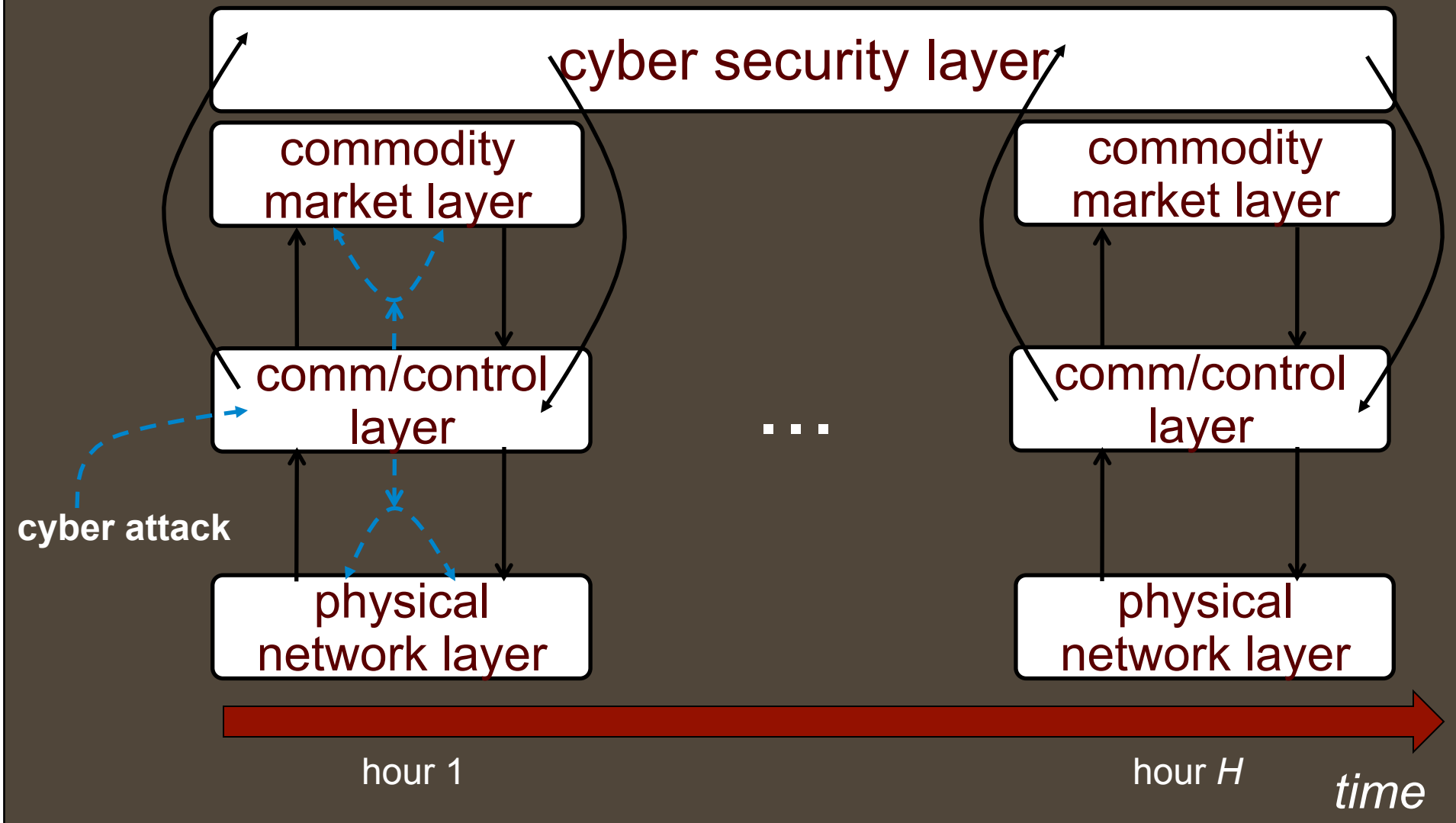
Hatch-power plant

- Who: Power plant engineer
- When: March, 2008
- What: An engineer at the Hatch power plant in Georgia installed a patch that rebooted a computer. Critical monitoring data was deleted, which was interpreted as a drop in reactor's cooling water, causing the plant to shut down for 48 hours.

Proposed Solution

- In order to better understand the problem, a conceptual four-layer framework is proposed
  1) Physical layer
  2) Communication/Control layer
  3) Market layer
  4) Cyber Security Investment layer
- Social welfare is used as a metric to quantify impacts of cyber attacks on the market layer

The Conceptual Framework



Physical Layer

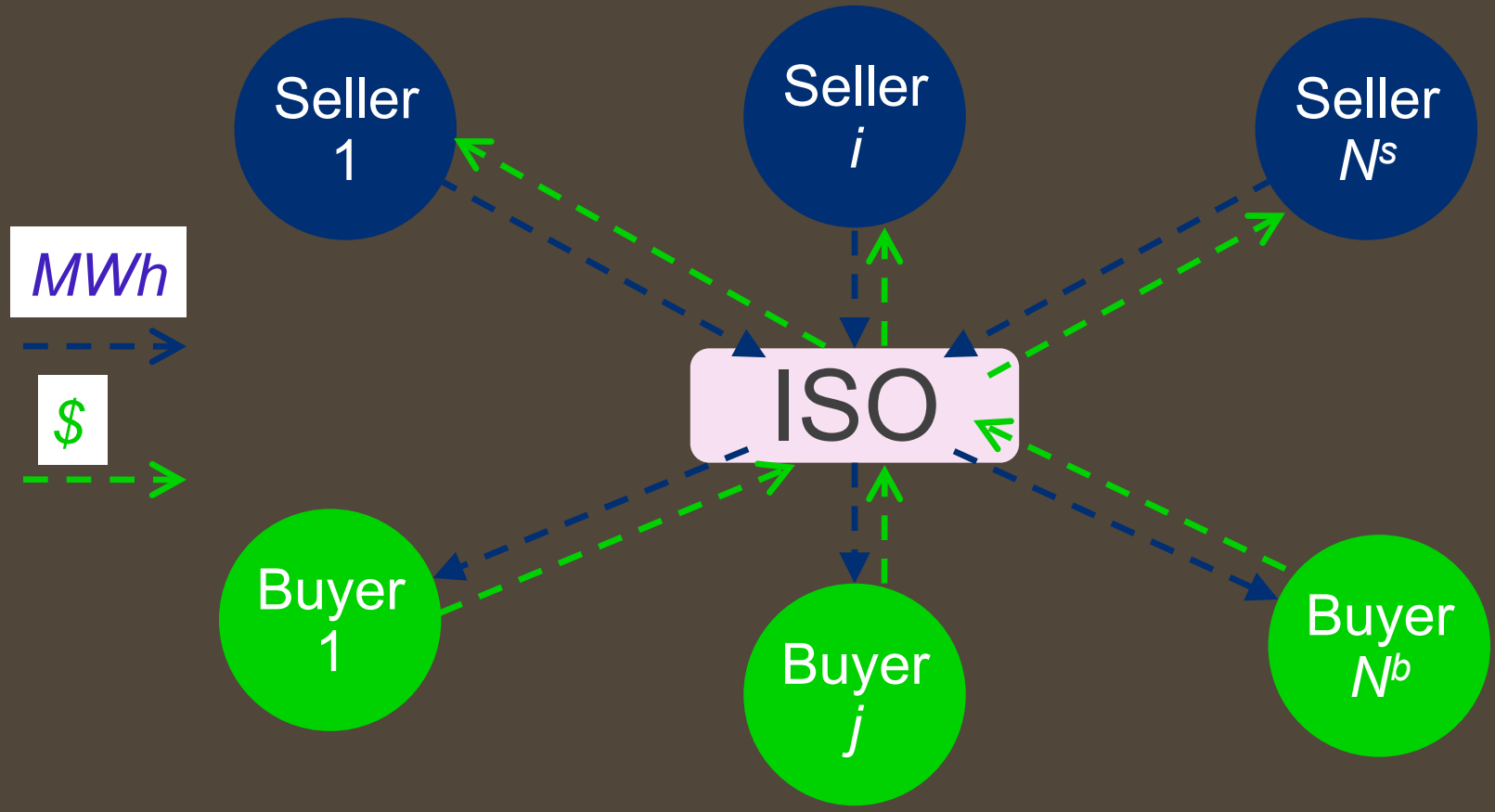
- Consists of the generation, transmission and distribution systems.
- Consider a system with *N*+1 buses and *L* lines
- $N \triangleq \{0, 1, 2, \ldots, N\}$ is the set of buses, with bus 0 being the slack bus
- $L \triangleq \{l_1, l_2, \ldots, l_L\}$ is the set of transmission lines that connect the *N+1* buses
- $l = (i, j)$ is an ordered pair of the set *L*
- The network flows are represented by the vector $\underline{f} = [f_1, f_2, \ldots, f_L]^T$
- System net power injections are represented by the vector $\underline{p} = [p_1, p_2, \ldots, p_N]^T$

Physical Layer, Cont'd

- Line series admittance of line *l* is represented by $Y_l = gl - jb_l$
- *L x L* diagonal branch susceptance matrix is defined by $\underline{\mathrm{B}}_d = diag\{b_1, b_2, \ldots, b_l\}$
- $\underline{\bar{\mathrm{A}}} \triangleq [\underline{\bar{\mathrm{a}}}_0, \underline{\bar{\mathrm{a}}}_1, \ldots, \underline{\bar{\mathrm{a}}}_L]$ is the augmented branch-to-node incidence matrix.
- Node-to-node susceptance matrix $\underline{\mathrm{B}} = \underline{\bar{\mathrm{A}}}^T \underline{\mathrm{B}}_d \underline{\bar{\mathrm{A}}}$
- Assuming a lossless power system, DC power flow equation is stated as $\underline{\mathrm{p}} = \underline{\mathrm{B}\theta}$
- Now, active line power flow limits are adopted as $\underline{\mathrm{B}}_d \underline{\mathrm{A}\theta} \leq \underline{\mathrm{f}}^{\max}$, where $\underline{\mathrm{A}}$ represents the reduced incidence matrix with the row/columns corresponding to the slack bus removed from the augmented incidence matrix $\underline{\bar{\mathrm{A}}}$

Commodity Market Layer

Centralized Electricity Market Structure: Players submit offers to sell energy to and bids to buy from the ISO



Commodity Market Layer, Cont'd

- Assumptions:
  - We have a competitive market (bids and offers reflect truthful costs and benefits).
  - There are at most one seller and one buyer at each node.
  - Market is cleared every hour.
- Bids and offers are represented by differentiable functions $v_n^b(p_n^b)$ and $\sigma_n^s(p_n^s)$
- The integral of these functions gives benefit and cost functions $B_n^b(p_n^b)$ & $C_n^s(p_n^s)$

Commodity Market Layer, Cont'd

- Vectors $\underline{\mathrm{p}}^{s} \triangleq [p_1^s, p_2^s, \ldots, p_N^s]^T$ & $\underline{\mathrm{p}}^{b} \triangleq [p_1^b, p_2^b, \ldots, p_N^b]^T$ contain information about selling and buying of energy at each node.
  - p_N^s - power injected at bus *N*
  - p_N^b - power withdrawn at bus *N*
- The market settlement for a particular hour results from maximization of social welfare.
  - The social welfare is a measure of the net benefits of both the sales and purchases.

Commodity Market Layer, Cont'd

- Optimization problem thus becomes:

$$\max s(p_0^s, p_0^b, \underline{p}^s, \underline{p}^b) = \sum_{n=0}^{N} \{B_n^b(p_n^b) - C_n^s(p_n^s)\}$$

- Such that:

$$p_0^s - p_0^b = \underline{b}_0^T \underline{\theta}$$

$$\underline{p}^s - \underline{p}^b = \underline{B\theta}$$

$$\underline{B}_d \underline{A\theta} \leq \underline{f}^{max}$$

Transmission constrained optimization problem (TCP)

Communication & Control Layer

- Consists of EMS and SCADA systems.
  - where SCADA is composed of Remote Terminal Units (RTUs) and master station connected through a communication network.
- Uses information from the market layer in order to manage the physical layer.
- Most vulnerable to cyber attacks as intensive data exchange takes place in this network.

Cyber Security Investment Layer

- Model upgrades to the communication and control layer to make it more secure, given the vulnerabilities and potential attacks.
  - Cyber attack example: opening of a breaker to cause topology change (may affect congestion).
- The investments are differentiated based on extent & scope of cyber security measures.
  - For example, different scopes of security investment could focus on confidentiality, availability or integrity of the system.

Cyber Security Investment Layer, Cont'd

TEXAS A&M UNIVERSITY

- Total social welfare for potential cyber attacks needs to be evaluated for every investment alternative over the time of study.

$$\max S = \sum_{h=1}^{H} \sum_{n=0}^{N} \{B_n^{b,h}(p_n^{b,h}) - C_n^{s,h}(p_n^{s,h})\}$$

- Such that:

$$p_0^{s,h} - p_0^{b,h} = \underline{b}_0^{hT} \underline{\theta}^h,$$

$$p_0^{s,h} - p_0^{b,h} = \underline{b}_0^{hT} \underline{\theta}^h, \qquad h = 1, 2, \ldots, H$$

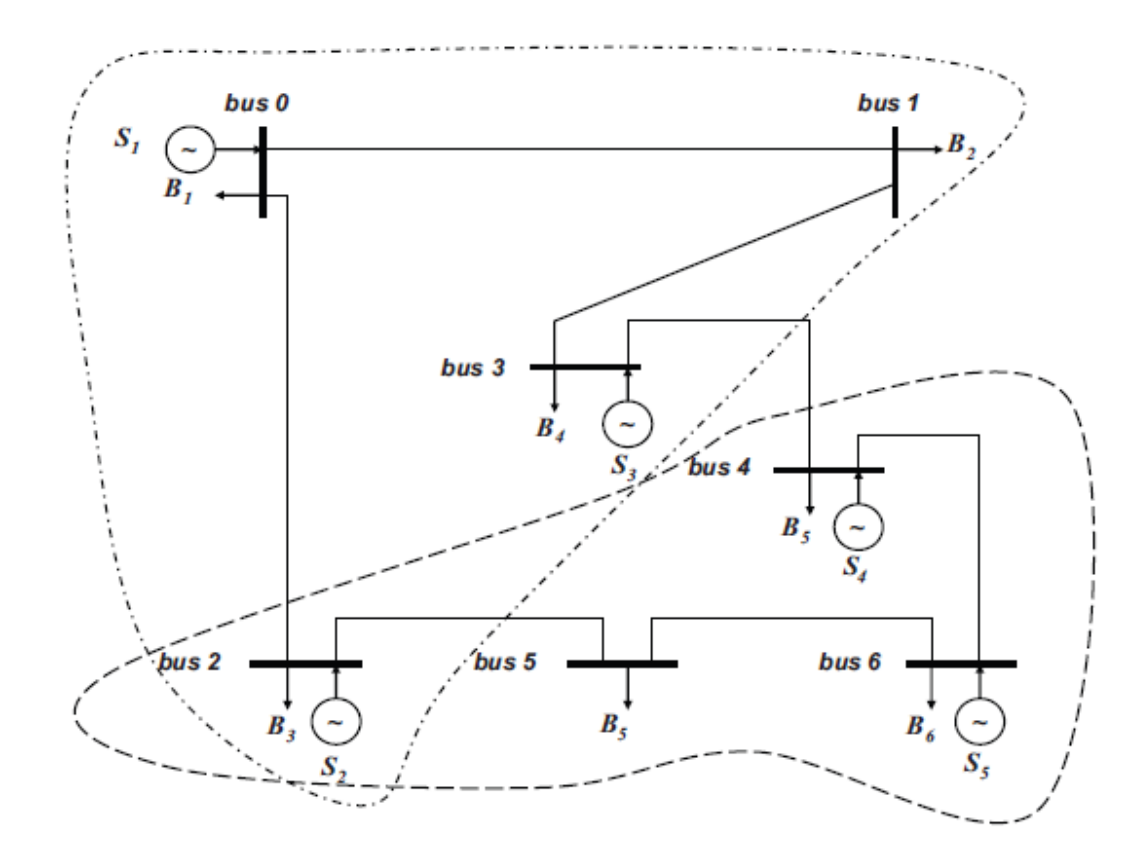
$$\underline{B}_d^h \underline{A}^h \underline{\theta}^h \leq \underline{f}^{\max}$$

Cyber Security Investment Layer, Cont'd

- In their illustration of the framework, authors:
  - differentiate investments using extent as a parameter.
  - use the opening of lines as the potential cyber attack.
- The set of lines associated with a cyber security investment layer are defined as $C \subseteq L$. It is assumed that these lines cannot be opened by remote attacks.
- Other line(s) which are not protected will be out-of service for a couple of hours after an attack.
  - $\underline{\mathbf{B}}^h$ and $\underline{\mathbf{A}}^h$ matrices therefore need to be updated during the study

Simulation Results

- 7-bus test system with 5 sellers and 7 buyers (shown is the system topology with two cyber secured areas).



Source: M. Negrete-Pincetic, F. Yoshida, and G. Gross. 2009

Simulation Results, Cont'd

- Impact of a cyber attack on the market and consequently social welfare are time variant.
- Equal probabilities are assigned for attacks on each season and during the on-peak/off-peak hours:
  - P(fall) = P(winter) = P(spring) = P(summer) = 0.25
  - P(on-peak) = P(off-peak) = 0.5

Note: There is not enough information available about real cyber attacks to statistically compute these probabilities

Simulation Results, Cont'd

- For each cyber security investment alternative *k*, expected social welfare is the metric associated with the selected cyber attack.
- $$\mathrm{E}(S^k) = \sum_{i=1}^{4}\sum_{j=1}^{2} \pi_{ij} \max\,(S^k)_{ij}$$
  - where $\max(S^k)_{ij}$ is the solution from the previously defined social welfare function S.
  - *i* is the season, and *j* is the time when selected cyber attack occurs
  - π_{ij} are the probabilities for a given scenario (0.125 in this case)
- Following quadratic functions are used for the benefit and cost functions:

$$B_n^{b,h}\left(p_n^{b,h}\right) = \beta_n^{b,h} p_n^{b,h} - \frac{1}{2}\gamma_n^{b,h}\left(p_n^{b,h}\right)^2$$

$$C_n^{s,h}\left(p_n^{s,h}\right) = \beta_n^{s,h} p_n^{s,h} + \frac{1}{2}\gamma_n^{s,h}\left(p_n^{s,h}\right)^2$$

Simulation Results, Cont'd

Table 1: Investment Alternatives

alternative	C
a	ø
b	(0, 2), (0, 1), (1, 3)
c	(2, 5), (5, 6), (6, 4)
d	*L*

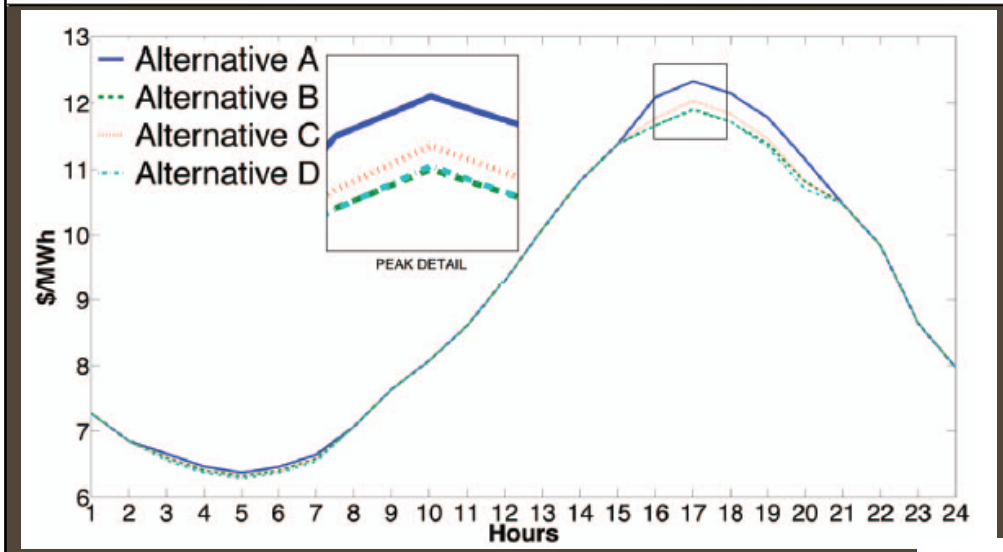
Table 2: Cyber Attacks

alternative	outage lines
a	(0, 1), (3, 4)
b	(4, 6)
c	(3, 4)
d	ø

Table 3: Total Social Welfare For Each Alternative

alternative	expected social welfare ($)
a	1925400
b	1927300
c	1927200
d	1928400

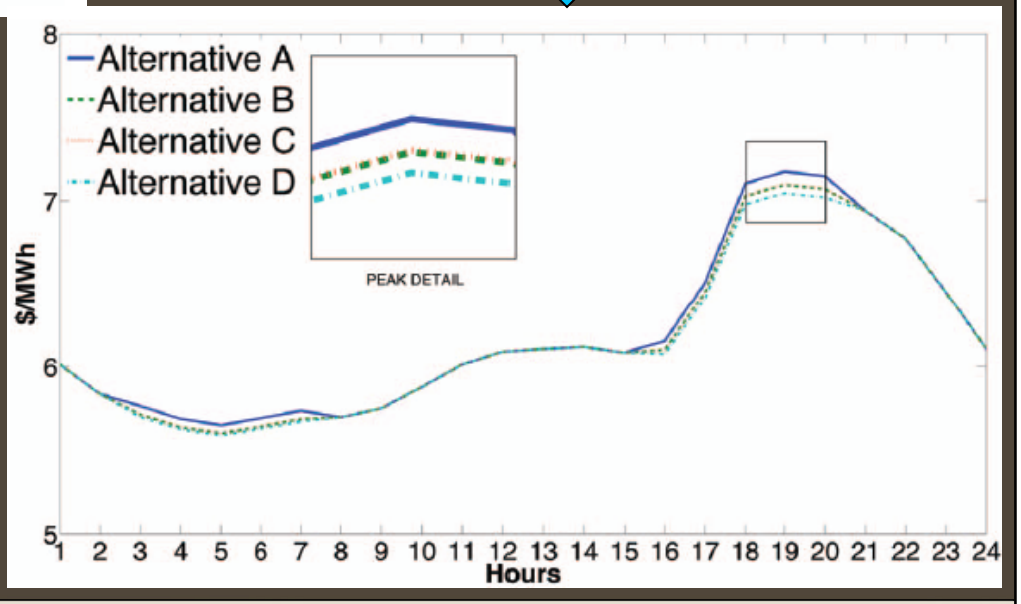
Simulation Results, Cont'd



Expected system LMPs summer attack.

- 96 hour study period was used, 24 hours for each season.
- System LMP (Locational Marginal Price) is computed by taking the average of the LMP at each bus.

Expected system LMPs winter attack.



Source: M. Negrete-Pincetic, F. Yoshida, and G. Gross. 2009

Pros and Cons

- Cyber attacks are characterized and real examples are given to emphasize the threats on the modern power grid.
- A suitable method is provided for quantifying the impacts of cyber attacks on the electricity market.
- However, detailed characterization of all components (hardware, software and communication) is required to accurately find vulnerabilities and determine potential cyber attacks.
- In this study, it is assumed that the lines associated with cyber security investment level cannot be remotely disconnected by attacks. It reality, however, no investment can guarantee 100% immunity.
- Critical subsets of lines and possibilities of cascading failures would need to be taken into account to get a more accurate estimate of the social welfare.

Conclusion and Future Work

- New communication capabilities add to already existing vulnerabilities in the grid.
- A four layer framework is proposed to understand the relation between various levels of the electricity market.
- Social welfare is used as a metric to quantify the impacts of cyber attacks.
- Future research would require a more detailed characterization of cyber attacks and to do this type of a study on a large scale scenario.

References

- M. Negrete-Pincetic, F. Yoshida, and G. Gross, “Towards quantifying the impacts of cyber attacks in the competitive electricity market environment,” Proceedings of IEEE PowerTech, Jul 2009.
- M. Liu, “A Framework for Transmission Congestion Management Analysis,” Ph.D.Thesis, Department of Electrical and Computer Engineering, University of Illinois at Urbana-Champaign, 2005.
- P. Caro-Ochoa, “Evaluation of Transmission Congestion Impacts on Electricity Markets,” M.S. Thesis, Department of Electrical and Computer Engineering, University of Illinois at Urbana-Champaign, 2003.

Thank You!

- Questions?